

UNITED STATES DISTRICT COURT

for the  
District of Oregon

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

Samsung Galaxy S21 Ultra, serial number  
RSCR10NL7NR, as described in Attachment A

Case No. 3:22-mc-86

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

Samsung Galaxy S21 Ultra, serial number RSCR10NL7NR, as described in Attachment A hereto,

located in the \_\_\_\_\_ District of \_\_\_\_\_ Oregon \_\_\_\_\_, there is now concealed (identify the person or describe the property to be seized):

The information and items set forth in Attachment B hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section  
18 U.S.C. §§ 242 and 1201

Offense Description  
Deprivation of Rights and Kidnapping

The application is based on these facts:

See affidavit which is attached hereto and incorporated herein by this reference.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Eric Hiser, Special Agent FBI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by  
Telephone at 2:37pm a.m./p.m. (specify reliable electronic means).

Date: January 25, 2022

City and state: Eugene, Oregon

  
Judge's signature

Mustafa T. Kasubhai, United States Magistrate Judge

Printed name and title

DISTRICT OF OREGON, ss: AFFIDAVIT OF ERIC HISER

**Affidavit in Support of an Application  
for a Search Warrant for a Phone**

I, Eric Hiser, being duly sworn, do hereby depose and state as follows:

**Introduction and Agent Background**

1. I am a special agent with the Federal Bureau of Investigation and have been since April 11, 2021. My current assignment is with the Portland Field Office on the White Collar Crimes squad, investigating financial crimes, and civil rights crimes, including sexual misconduct committed under color of law in violation of 18 U.S.C. § 242. My training and experience includes specialized training received at the FBI Academy in Quantico, Virginia, related to investigative and legal matters including guidance on conducting searches of computers, cell phones, and electronic devices. I previously worked as a forensic accountant from 2016 to 2020 in the FBI's Philadelphia Division, where I assisted FBI special agents with the preparation of search warrant affidavits related to organized crime, money laundering, and fraud. Additionally, I have conducted or participated in surveillance operations, assisted in the execution of search warrants and arrest warrants, and reviewed records as part of my investigations.

2. I submit this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the search and examination of a Samsung Galaxy S21 Ultra, serial number RSCR10NL7NR, (hereinafter "Phone"), which is currently in law enforcement custody at 1201 NE Lloyd Boulevard, Portland, Oregon 97232, as described in Attachment A hereto, and the extraction of electronically stored information from

the Phone, as described in Attachment B hereto. As set forth below, I have probable cause to believe and do believe that the items set forth in Attachment B constitute evidence of violations of 18 U.S.C. §§ 242 (Deprivation of Rights) and 1201 (Kidnapping).

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers, interviews of witnesses, a review of records related to this investigation, communications with others who have knowledge of the events and circumstances described herein, and information gained through my training and experience.

#### **Applicable Law**

4. Title 18, United States Code, Section 242 provides that:

Whoever, under color of any law, statute, ordinance, regulation, or custom, willfully subjects any person in any State, Territory, Commonwealth, Possession, or District to the deprivation of any rights, privileges, or immunities secured or protected by the Constitution or laws of the United States, or to different punishments, pains, or penalties, on account of such person being an alien, or by reason of his color, or race, than are prescribed for the punishment of citizens, shall be fined under this title or imprisoned not more than one year, or both; and if bodily injury results from the acts committed in violation of this section or if such acts include the use, attempted use, or threatened use of a dangerous weapon, explosives, or fire, shall be fined under this title or imprisoned not more than ten years, or both; and if death results from the acts committed in violation of this section or if such acts include kidnapping or an attempt to kidnap, aggravated sexual abuse, or an attempt to commit aggravated sexual abuse, or an attempt to kill, shall be fined under this title, or imprisoned for any term of years or for life, or both, or may be sentenced to death.

5. Title 18, United States Code, Section 1201 provides in relevant part that:

(a) Whoever unlawfully seizes, confines, inveigles, decoys, kidnaps,

abducts, or carries away and holds for ransom or reward or otherwise any person, except in the case of a minor by the parent thereof, when—

(1) the person is willfully transported in interstate or foreign commerce, regardless of whether the person was alive when transported across a State boundary, or the offender travels in interstate or foreign commerce or uses the mail or any means, facility, or instrumentality of interstate or foreign commerce in committing or in furtherance of the commission of the offense;

\*\*\*\*

shall be punished by imprisonment for any term of years or for life and, if the death of any person results, shall be punished by death or life imprisonment.

### **Statement of Probable Cause**

6. In November 2021, the Oregon State Police (OSP) began investigating allegations that Zakary Glover (“Glover”), while serving in his capacity as a Direct Support Crisis Specialist for the Oregon Department of Human Services Stabilization and Crisis Unit (SACU), sexually assaulted Adult Victim 1 (“AV1”), a 28-year-old female patient in his care. In December 2021, OSP contacted the FBI for assistance, and the FBI commenced a federal investigation.<sup>1</sup> I am the case agent assigned to the ongoing federal investigation.

7. At all relevant times, Glover worked as a State of Oregon employee in his position as a Direct Support Crisis Specialist with SACU. SACU is a 24-hour crisis residential program in Marion County, Oregon, that services individuals with intellectual and developmental disabilities who require constant care.

8. AV1 is civilly committed to SACU. AV1 has significant cognitive disabilities,

---

<sup>1</sup> Glover has been charged by indictment by the State of Oregon for violations of state statutes related to his conduct in this matter. *See State v. Glover*, 21CR58456. He is currently being detained without bond pending trial.

autism, epilepsy, and barely communicates verbally. For example, if AV1 is hungry, she points to a picture of the food she wants to eat. She often watches YouTube videos for entertainment. Although AV1 can feed and dress herself, she needs assistance bathing and going to the bathroom. She is also prone to biting and attacking others.

9. On November 2, 2021, Glover was assigned to take AV1 to a Taco Bell drive-thru, an occasional outing that she is permitted. Glover transported AV1 in a secure van, owned by the Oregon Department of Administrative Services and assigned to SACU. The secured van has passenger doors that cannot be opened from the inside and a dividing partition of heavy plastic between the front and rear seats. AV1 was being transported in the rear secured area for her safety and the safety of others.

10. During the transport, Glover drove AV1 to a secluded trail adjacent to the Aumsville Cemetery on Steinkamp Road in Marion County, Oregon. Based on the investigation to date, there was no legitimate purpose for Glover to drive to the cemetery.

11. A surveillance video camera at the Aumsville Cemetery captured a clear, unobstructed view of Glover and of the van, and much of his conduct thereafter that forms the basis of the subsequent investigation.

12. About six days after the incident, a cemetery caretaker who routinely reviews surveillance footage of the trail outside the cemetery gate discovered footage of the incident and reported it to state authorities.

13. The videos show Glover's van make a three-point turn in front of the cemetery's gate and park the van facing the camera. Glover rolls down the rear passenger window before exiting the vehicle. Based on records and accounts from staff at SACU, I confirmed that AV1

was the only passenger in the vehicle.

14. The video shows Glover, with his Phone in hand, walking around the front of the van and approaching the rear passenger window. Glover leans into the open window with the Phone, appearing to show the screen of the Phone to AV1. The Phone's screen is not visible due to the reflection of the windshield and the interior partition separating the driver's compartment from the rear passenger area.

15. Glover then makes a "come here," beckoning motion with his left hand. With the Phone still in his right hand, Glover then makes another motion with both hands as if he is miming lifting up his shirt to AV1. Glover opens the sliding rear passenger door, appears to slide the Phone into his pocket, and leans into the cabin with his feet outside the vehicle on the ground. The vehicle shakes as if someone is moving around inside the van. Glover then stands up. He pulls down his shorts and underwear to just above the knee, so that is bare buttocks is visible. The video does not show Glover's penis due to the position of the camera and his body.

16. Glover then moves up against the van with both his hands in the cabin. He sucks one of his fingers, takes a half step back, and then puts both his arms inside the vehicle. Glover starts jerking his right arm back and forth rapidly, and then thrusts his lower body into the vehicle. He backs up, licks a finger on his right hand, and then again puts both arms inside the cabin. Glover thrusts again and then licks his finger for the third time. Glover continues to thrust his body into the van.

17. Glover then steps back, pulling AV1's feet out of the van by the ankles. AV1's sneakers and legs are briefly visible on the video. Glover pulls AV1's ankles up, presumably over her head, and AV1's feet and legs disappear from view. Glover then resumes thrusting

into the van with his shorts at his knees and his buttocks exposed. AV1 makes several loud noises as Glover licks his finger again and puts his arm into the van and out of the view of the camera. Glover alternates between rapidly jerking his right arm and thrusting back and forth into the van. At times, the thrusting is enough to shake the entire van.

18. Glover then pulls back and AV1 makes another loud sound. Glover then rapidly jerks his right arm again, stops, and stands while pulling up his shorts. A blanket or coat can be seen spilling out of the open door right in front of where Glover was standing. AV1 pulls the item back into the van while Glover stands and appears to say something to AV1 that is not loud enough to hear. Glover pulls the rear passenger door shut and gets back into the driver's seat. He rolls up the back window and drives away.

19. As part of its investigation, OSP searched the SACU van in question and located a SACU-issued cell phone. Investigation determined that the SACU phone is stored in the van and available for use by employees who are driving the van. The SACU phone was a black iPhone in a blue case, with the phone number and pin access code written on the back of the phone case. OSP, with the consent of the SACU, did a physical search of the that phone. The OSP detective determined that on November 2, 2021, there were no outgoing or incoming phone calls or text messages made or received, there was no browsing history on the work phone, and there were no photos or videos. Additionally, there was no YouTube app on the work phone.<sup>2</sup> According to the OSP detective, the SACU phone appeared as if it is very seldom used.

---

<sup>2</sup> Apps is an abbreviation for applications. An app is a self-contained program or piece of software designed to fulfill a particular purpose. An app can run on the Internet, on a computer, on a cell phone, or on other electronic devices.

20. On November 30, 2021, OSP interviewed Glover at his residence. The detective summarized what the trail camera video captured, and specifically mentioned that Glover showed his phone to AV1 through an open window.<sup>3</sup> Glover explained that AV1 gets upset if he veers from the route to Taco Bell, so he showed her a photo of a burrito through the window in an effort to calm her down. Just as the detective told Glover that he would be placed under arrest, Glover's cell phone began ringing. Glover said that he needed to get his phone from another room. The detective accompanied Glover to get his phone, a black Samsung Galaxy S21 Ultra cell phone, the subject Phone. The detective observed that the Samsung Galaxy that Glover used looked like the phone shown in the trail camera video – different than the SACU iPhone.

21. On January 24, 2022, I interviewed Glover's spouse, referred to within as Witness 1 (W1). She stated that she texted Glover throughout the day on November 2, 2021, on his Phone. She further stated that Glover responded quickly to all W1's messages without any unusual breaks in responses. W1 knew that Glover did not have a work phone and only used one phone, his Samsung Galaxy.

22. OSP seized the Phone from Glover during the arrest, and subsequently swore out an affidavit in support of a warrant to search the Phone. On December 7, 2021, The Honorable Lindsay Partridge of the Marion County Circuit Court issued the warrant. The Phone is currently in the custody of the FBI's Regional Computer Forensics Laboratory at 1201 NE Lloyd Boulevard, Portland, Oregon 97232. In my training and experience, I know that the Phone has

---

<sup>3</sup> Several times before stating that he "needs to talk to an attorney," Glover mentions that his union representative told him that he should get a lawyer.

been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Phone first came into the possession of the OSP.

### **Use and Purpose of a Cellular Phone**

23. Based on my training and experience, a wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and email; taking, sending, receiving, and storing still photographs and moving video; recording, storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet,<sup>4</sup> including the use of apps. Wireless telephones may also include a global positioning system (“GPS”) technology for determining the location of the device.

24. Based on my training, experience, and research, I know that the Phone has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player,

---

<sup>4</sup> The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

GPS navigation device, and Internet browser. In my training and experience, examining data stored on wireless telephones can uncover, among other things, evidence that reveals or suggests who possessed or used the phone, how the phone was used, and the purpose of its use.

25. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant but also forensic evidence that establishes how the Phone was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence will be on the Phone because, based on my knowledge, training, and experience, I know:

a. Phones can store information for long periods of time, including information viewed via the Internet. Files or remnants of files can be recovered with forensic tools months or even years after they have been downloaded onto a phone, deleted, or viewed via the Internet. Electronic files downloaded to a phone can be stored for years at little or no cost. When a person “deletes” a file, the data contained in the file does not actually disappear, rather that data remains on the phone until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the phone that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, the operating system may also keep a record of deleted data.

b. Wholly apart from user-generated files, the Phone may contain electronic evidence of how it has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating systems or application operations, and file system data structures.

c. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

d. Data on the Phone can provide evidence of a file that was once on the Phone but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Systems can leave traces of information on the Phone that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the Phone that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, including SD cards or other flash media, and the times the Phone was in use. File systems can record information about the dates files were created and the sequence in which they were created.

e. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

f. A person with appropriate familiarity with how the Phone works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how the Phone was used, the purpose of its use, who used it, and when.

g. The process of identifying the electronically stored information necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on the Phone is evidence may depend on other information stored on the Phone and the application of knowledge about how a Phone functions. Therefore, contextual information

necessary to understand other evidence also falls within the scope of the warrant.

h. Further, in order to find evidence of how the Phone was used, the purpose of its use, who used it, and when, the examiner may have to establish that a particular thing is not present on the Phone.

### **Nature of Examination**

26. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Phone consistent with the warrant. The examination may require authorities to employ techniques, including imaging the Phone and computer-assisted scans and searches of the entire Phone that might expose many parts of the device to human inspection in order to determine whether it constitutes evidence as described by the warrant.

27. The initial examination of the Phone will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

28. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the Phone or image do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data

falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

29. If an examination is conducted, and it is determined that the Phone does not contain any data falling within the ambit of the warrant, the government will return the Phone to its owner within a reasonable period of time following the search and will seal any image of the Phone, absent further authorization from the Court.

30. If the Phone contains evidence, fruits, contraband, or is an instrumentality of the crime, the government may retain the Phone as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the Phone and/or the data contained therein.

31. The government will retain a forensic image of the Phone for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

#### **Manner of Execution**

32. Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

**Conclusion**

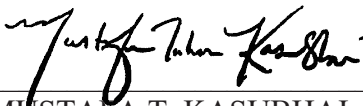
33. Based on the foregoing, I have probable cause to believe, and I do believe, that the Phone described in Attachment A contains evidence of violations of 18 U.S.C. §§ 242 and 1201, as set forth in Attachment B. I therefore request that the Court issue a warrant authorizing a search of the Phone described in Attachment A for the items listed in Attachment B and the seizure and examination of any such items found.

34. Prior to being submitted to the Court, this affidavit, the accompanying application, and the requested search warrant were all reviewed by Assistant United States Attorney Gavin Bruce of the District of Oregon, Special Litigation Counsel Fara Gold and Trial Attorney Daniel Grunert of the Civil Rights Division of the U.S. Department of Justice. They advised me that in their opinion the affidavit and application are legally and factually sufficient to establish probable cause to support the issuance of the requested warrant.

/s/ Eric Hiser, Per rule 4.1

\_\_\_\_\_  
Eric Hiser  
Special Agent, FBI

Sworn in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone at 2:38pm  
a.m/p.m. on January 25, 2022 .

  
\_\_\_\_\_  
MUSTAFA T. KASUBHAI  
United States Magistrate Judge

**ATTACHMENT A**

The property to be searched is a Samsung Galaxy S21 Ultra, serial number RSCR10NL7NR, hereinafter the “Phone”. The Phone is currently in law enforcement custody at 1201 NE Lloyd Boulevard, Portland, Oregon 97232.

**ATTACHMENT B**

1. All records on the Phone described in Attachment A that relate to violations of 18 U.S.C. §§ 242 and 1201 and Zakary Glover since November 2, 2021, including:
  - a. All records of communications sent or received by the Phone, including but not limited to emails, text messages, voicemails, recorded calls, chat messages, and saved drafts of any of the above;
  - b. All photos and videos saved or maintained on the Phone;
  - c. All records, content, and other information stored by an individual using the Phone related to the use of YouTube, including images, videos, and all files;
  - d. Information recording Glover's location or travel;
  - e. Evidence of user attribution showing who used or owned the Phone, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.
  - f. Records evidencing the use of the Internet, including:
    - i. Records of Internet Protocol addresses used.
    - ii. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.
  - g. Any deleted records, content, or other information described in subparagraphs a and f, above;
2. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or

stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

### **Search Procedure**

3. The examination of the Phone may require authorities to employ techniques, including imaging the Phone and computer-assisted scans and searches of the entire Phone that might expose many parts of the Phone to human inspection in order to determine whether it constitutes evidence as described by the warrant.

4. The initial examination of the Phone will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

5. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the Phone or image do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

///

6. If an examination is conducted, and it is determined that the Phone does not contain any data falling within the ambit of the warrant, the government will return the Phone to its owner within a reasonable period of time following the search and will seal any image of the Phone, absent further authorization from the Court.

7. If the Phone contains evidence, fruits, contraband, or is an instrumentality of a crime, the government may retain the Phone as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the Phone and/or the data contained therein.

8. The government will retain a forensic image of the Phone for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

- a. records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

9. As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

10. This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.